

Insider Threat Awareness



Combating the ENEMY
Within

*Mr. Richard Barnard
Command Security Manager
MCIEAST-MCB Camp Lejeune*

Insider Threat Awareness

- What is an Insider Threat?
- Indicators of Insider Threat
- General Suspicious Behaviors
- Reporting Potential Insider Threats
- Self-Graded Examination



What is an Insider Threat?

- A person using his or her authorized access, wittingly or unwittingly, to do harm to the national security and industry.

Insider Threats also include:

- Criminal activity – including theft and fraud
- Safety – including active shooter incidents
- Financial harm to industry – stealing unclassified, but sensitive or proprietary information

Results of Insider Threats:

- Loss/compromise of classified, export controlled, or proprietary information
- Weapons systems cloned, destroyed, or countered
- Loss of technological superiority
- Economic loss
- Loss of life



First Line of Defense – YOU!

Recognizing and Reporting Potential Insider Threats:

- Recruitment
- Information Collection
- Information Transmittal
- General Suspicious Behaviors



Insider Threat Indicators

Recruitment

- Unreported request for critical assets outside official channels
- Unreported or frequent foreign travel
- Suspicious foreign contacts
- Contact with individuals known or suspected to be associated with foreign intelligence, security, or terrorism
- Unreported offers of financial assistance, gifts, or favors by foreign national or stranger
- Suspected recruitment of employee by foreign or domestic competitive companies

Insider Threat Indicators (cont.)

Information Collection

- Using unclassified medium to transmit classified materials
- Discussing classified materials on a non-secure telephone
- Removing classification markings from documents
- Unauthorized downloading or copying of files
- Keeping classified materials/critical assets in unauthorized locations
- Attempting to or accessing sensitive information, critical assets, or information systems when not required or without authorization
- Asking others to obtain critical assets to which the requestor does not have authorized access
- Operating unauthorized cameras, recording devices, computers, or modems where critical assets are stored/discussed/processed

Insider Threat Indicators (cont.)

Information Transmittal

- Removing critical assets from the work area without authorization
- Extensively reproducing/transmitting critical asset-related information beyond job requirements
- Discussing critical asset-related information in public or on a non-secure telephone
- Using an unauthorized fax or computer to transmit classified information
- Attempting to conceal foreign travel – business or personal
- Improperly removing classification markings from documents

General Suspicious Behaviors

- Attempts to expand access to critical assets by repeatedly volunteering for duties beyond normal job responsibilities
- Performs repeated or unrequired work outside of normal hours, especially unaccompanied
- Repeated security violations
- Engagement in illegal activity or requesting others to do so
- Unexplained or undue affluence explained by inheritance, luck in gambling, or some business venture
- Sudden reversal of financial situation or repayment of large debts

General Suspicious Behaviors (cont.)

- Attempts to compromise personnel with access to critical assets special treatment, favors, gifts, money or other means
- Displays questionable loyalty to U.S. Government or company
- Behaviors associated with disgruntled employees:
 - Conflicts with supervisors and coworkers
 - Decline in work performance
 - Tardiness
 - Unexplained absenteeism



If you suspect a potential Insider Threat You MUST report it!

- Contact your:
 - MCIEAST Security Manager, Mr. Richard Barnard
 - e-mail: richard.barnard@usmc.mil
 - phone: 910-451-3568/3563

Failure to Report

- Risks YOUR physical security, the Information Security of your organization, and the security of the United States!
- Risks YOU:
 - Losing your security clearance
 - Losing your employment
 - Facing possible criminal charge



**Remember -
YOU are the First Line of Defense!**

**If you suspect a potential Insider
Threat,
You must report it!**



Actual Occurrences of Insider Threats

- **DSS Counterintelligence Reports**
 - http://www.dss.mil/isp/count_intell/ci_reports.html
- **DHS US CERT and FBI**
 - <http://www.fbi.gov/news/stories/story-index/cyber-crimes>
 - [https:// www.cert.org/insider-threat/](https://www.cert.org/insider-threat/)

Q&A

- General comments about the video... Do you believe it provided some insight into the various elements involved with the Insider Threat?
- How do you believe this person was recruited?
- What were some of the suspicious behaviors observed by the co-workers that indicated something wasn't right?
- Could something like this happen to By Light? How/Why?
- What do you believe was the end result for the other team members?